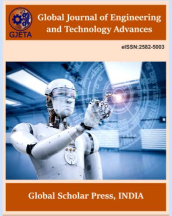
GJETA

Global Journal of Engineering and Technology Advances

eISSN: 2582-5003

Cross Ref DOI: 10.30574/gjeta

Journal homepage: https://gjeta.com/


Global Journal of Engineering and Technology Advances
GJETA
eISSN:2582-5003
Global Scholar Press, INDIA

(Review Article)

Subject review: Image encryption techniques

Wedad Abdul Khuder Naser *, Amal Abbas Kadhim and Safana Hyder Abbas

Department of computer science, University Al Mustansiriyah, Baghdad, Iraq.

Global Journal of Engineering and Technology Advances, 2023, 15(03), 029–031

Publication history: Received on 20 April 2023; revised on 02 June 2023; accepted on 05 June 2023

Article DOI: https://doi.org/10.30574/gjeta.2023.15.3.0098

Abstract

Security is one of the core areas of study in recent days. Encryption of the image is widely known as an effective method for its secure transmission. The objective of any image encryption method is to obtain a top quality hidden image in order to keep information secret. This paper is a study of research authors in the field of image encryption with a research review to see how the field of image encryption has progressed and the best algorithms in their performance.

Keywords: Image Encryption; Chaotic Algorithms; Encryption; Decryption; Security Parameters

1. Introduction

With the ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images, and encryption is one the ways to ensure security. Image encryption techniques try to convert original image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption. Furthermore, special and reliable security in Storage and transmission of digital images is needed in many applications, such as cable-TV, online personal photograph album, medical imaging systems, military image communications and confidential video conferences, etc. In order to fulfill such a task, many image encryption methods have been proposed. [1.2]. In general, a well-studied, fast and secure conventional cryptosystem should be chosen, surely those algorithms, which provides higher security

1.1. Survey of literature

Many image encryption techniques have been developed by researchers and scientists, some of the most important and widely used image encryption techniques are shown below.

In this paper, analyze the Advanced Encryption Standard (AES), and in their image encryption technique they add a key stream generator (A5/1, W7) to AES to ensure improving the encryption performance [3].

In this paper, proposed a novel algorithm for image encryption based on SHA-512 hash function. The algorithm consists of two main sections: The first does preprocessing operation to shuffle one half of image. The second uses hash function to generate a random number mask. The mask is then XORed with the other part of the image which is going to be encrypted [4].

In this paper, The traditional chaotic model is utilized in the encryption calculation to produce two arrangements of chaotic groupings to encrypt the image, The two-layered model is utilized to create turbulent groupings to encode and scramble the image. Through the security examination, it very well may be presumed that the image encryption calculation proposed is delicate to the mystery key and has an enormous mystery key space. It can oppose thorough

* Corresponding author: Wedad Abdul Khuder Naser

assaults to a serious level and can oppose clamor obstruction. The calculation has solid security and heartiness and is reasonable for image encryption with high security level [5].

In this paper, Consolidating logistic map with increasingly in digit stage activities. Encryption calculation uses both increasingly in piece stage to scramble pixels. Besides, chaotic diffusion is additionally performed to additional protected images. The sensitive boundaries of strategic guide make the key space adequately enormous enough to oppose beast power assault. The quantum circuits are given and mathematical reproduction results show that the proposed conspire is secure to oppose different assaults. The computational intricacy of the proposed plot is lower than traditional image encryption [6].

In this paper, The proposed conspire has preferable execution over the regular one as far as the pressure execution. Test results showed that images scrambled by utilizing the proposed plot had a higher-pressure execution than those encoded by the traditional grayscale plan. Also, the proposed plot was affirmed to have practically a similar strength against ciphertext-just assaults as the regular grayscale-based encryption [7].

In this paper, The proposed scheming comprises of three phases confusion rearranging and diffusion. In disarray the first image is befuddled by utilizing Arnold feline turbulent guide. the pixels of the befuddled picture are rearranged to add more irregularity and unconventionality. the rearranged picture is diffused by a key picture created by consolidating arrangements produced from Henon and Strategic chaotic maps[8].

In this paper, proposed new image encryption technique based on new chaotic system by adding two chaotic systems: the Lorenz chaotic system and the Rössler chaotic system. From Experimental analysis they demonstrate that the image encryption algorithm has the advantages of large key space and high-level security, high obscure level and high speed [9].

In this paper, proposed a new method based on a hybrid model composed of a genetic algorithm and a chaotic function for image encryption. In their technique, first a number of encrypted images are constructed using the original image with the help of the chaotic function. In the next stage, these encrypted images are employed as the initial population for starting the operation of the genetic algorithm. Then, the genetic algorithm is used to optimize the encrypted images as much as possible. In the end, the best cipher-image is chosen as the final encryption image [10].

In this paper, taking advantage of chaotic systems and neural networks by combining them into a single platform for image encryption. The input image is fed into a chaotic neural layer in which methods like Chua and Liu systems are employed to bring the chaotic behavior. The output is then fed into a permutation neural network where a nonlinear mapping is performed to obtain the final encrypted output. The decryption phase is the inverse of the encryption phase. The entropy of the resulting image is high, and the histograms of the original and encrypted image bear no resemblance. The only limitation of this method is that it is difficult to implement [11].

In this paper, uses Elliptic Curve and AES encryption. AES encryption is performed in multiple rounds. Each round has four main steps that include byte substitution, row shifting, column mixing and the addition of round key. In the round key step, the output matrix of mix column is XOR-ed with round key. The security of elliptic key cryptography is promised by a discrete logarithmic problem. In the beginning, the sender and receiver compromise on a standard (Elliptic Curve Cryptography) ECC. Once random numbers are generated using the elliptic curve, they are used for creating a group of masked matrices for encryption. Each bit of the current image is XOR-ed with each bit of the masker. This method is resistant to statistical and differential attack [12].

In this paper, uses cellular automata, Linear feedback shift register and synthetic image. Permutation and Diffusion are both provided by Cellular automata. The work of a pseudo-random generator is provided by the linear feedback shift register. An important thing about linear feedback shift register is that its output depends on its past state. Cellular automation is very easy to construct because of which it finds an application in many real systems. Synthetic image accounts as a collector of keys. Every next stage of the linear feedback shift register is XORed with the current stage at the rising clock edge to obtain the encrypted image. The encrypted image has high entropy and the correlation coefficients of the adjacent pixels are far apart. This method thus proves to be an efficient method for image encryption [13].

In this paper, introduces an efficient chaos-based stream cipher, composing two chaotic logistic maps and a large enough external secret key for image encryption[14].

2. Conclusion

In this paper, we have surveyed existing work on image encryption. We conclude that all techniques are effective for real-time picture encryption. Techniques that can offer security features and a general visual examination are described in this paper and may be appropriate in some situations. Therefore, no one can access a image that is sent over an open network. In general, a well-studied, fast and secure conventional cryptosystem should be chosen, surely those algorithms, which provides higher security. Based on a careful examination of all of the above-mentioned researchs: chaotic method demonstrates a high degree of uncertainty and offers a very high level of safety.

Compliance with ethical standards

Acknowledgments

The authors would like to thank the Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad, Iraq for supporting this work.

Disclosure of conflict of interest

All authors declare that they have no conflict of interest

References

[1] Aloha Sinha, Kehar Singh, A technique for image encryption using digital signature, Optics Communications, Vol-2 I 8 (2203), 229-234.

[2] S.S.Maniccam, N.G. Bourbakis, Lossless image compression and encryption using SCAN, Pattern Recognition 34 (2001), 1229- 1245.

[3] M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki, A Modified AES Based Algorithm for Image Encryption, World Academy of Science, Engineering and Technology 27, 2007.

[4] Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki, A Novel Image Encryption Algorithm Based on Hash Function 6th Iranian Conference on Machine Vision and Image Processing, 2010.

[5] Li, T., Du, B. and Liang, X., Image encryption algorithm based on logistic and two-dimensional Lorenz. 2020, IEEE Access, 8, pp.13792-13805.

[6] Liu, X., Xiao, D. and Xiang, Y., Quantum image encryption using intra and inter bit permutation based on logistic map, 2018, IEEE Access, 7, pp.6937-6946.

[7] Sirichotedumrong, W. and Kiya, H., Grayscalebased block scrambling image encryption using ycbcr color space for encryption-then-compression systems. APSIPA Transactions on Signal and Information Processing, 2019. 8.

[8] Abdullah, H.N. and H.A. Abdullah. Image encryption using hybrid chaotic map. in 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT). 2017. IEEE.

[9] Qais H. Alsafasfeh, Aouda A. Arfoa,Image Encryption Based on the General Approach for Multiple Chaotic Systems, Journal of Signal and Information Processing, 2011.

[10] Rasul Enayatifar, Abdul Hanan Abdullah, Image Security via Genetic Algorithm, International Conference on Computer and Software Modeling IPCSIT, 2011, vol.14.

[11] S H Kamali, R Shakerian, M Hedayati, M Rahmani, A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption, ICEIE Conference, Year: 2010, Volume:1 Pages: 141–145.

[12] Shahryar Toughi, Mohammad H. Fathi, Yoones A. Sekhavat, An image encryption scheme based on elliptic curve pseudo-random and Advanced Encryption System, Volume 141, December 2017, Pages 217–227.

[13] S Rajagopalan, S Rethinam, S Janakiraman, Har Narayan Upadhyay, R Amirtharajan, Cellular Automata + LFSR + Synthetic image: A trio approach to image encryption, ICCI conference, Year: 2017 Pages: 1 – 6.

[14] Ismail Amr Ismail, Mohammed Amin, Hossam Diab A Digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps, International Journal of Network Security, July 2010, Vol.11, No.1, PP.1 -10.